OWASP SAMM Best Practices, Lessons from the Trenches

Seba Deleersnyder
seba@owasp.org

OpenSAMM project co-leader

presentation created together with Bart De Win for AppSecEU14
OWASP Germany 2014 Talk
Sebastien Deleersnyder

15+ years developer / information security experience
Belgian OWASP chapter founder
OWASP volunteer
Co-organizer www.BruCON.org

Co-Founder & Application security specialist Toreon

be.linkedin.com/in/sebadele/
Agenda

• Integrating software assurance?
• OWASP SAMM
• Quick start
• Lessons learned
• Resources & self-assessment
• OWASP SAMM – get involved
“Build in” software assurance

Secure Development Lifecycle (SAMM)

- Proactive
  - Security requirements / threat modeling
  - Coding guidelines
  - Code reviews
  - Static test tools

- Reactive
  - Security testing
  - Dynamic test tools
  - Vulnerability scanning - WAF

Stages:
- Design
- Build
- Test
- Production
We need a Maturity Model

Changes must be iterative while working toward long-term goals. A solution must enable risk-based choices tailored to the organization. A solution must provide enough details for non-security people. 

Guidance related to security activities must be prescriptive. 

Must be simple, well-defined, and measurable. 

There is no single recipe that works for all organizations. A solution must enable risk-based choices tailored to the organization. 

An organization's behavior changes slowly over time. There is no single recipe that works for all organizations. 

Guidance related to security activities must be prescriptive. 

Must be simple, well-defined, and measurable. 

We need a Maturity Model.
SAMM users

- Dell Inc
- KBC
- ING Insurance
- Gotham Digital Science
- HP Fortify
- ISG ...
SAMM Security Practices

- From each of the Business Functions, 3 Security Practices are defined
- The Security Practices cover all areas relevant to software security assurance
- Each one is a ‘silto’ for improvement
## Example: Education & Guidance

<table>
<thead>
<tr>
<th>Objective</th>
<th>EG 1</th>
<th>EG 2</th>
<th>EG 3</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Objective</strong></td>
<td>Offer development staff access to resources around the topics of secure programming and deployment</td>
<td>Educate all personnel in the software life-cycle with role-specific guidance on secure development</td>
<td>Mandate comprehensive security training and certify personnel for baseline knowledge</td>
</tr>
<tr>
<td><strong>Activities</strong></td>
<td>A. Conduct technical security awareness training B. Build and maintain technical guidelines</td>
<td>A. Conduct role-specific application security training B. Utilize security coaches to enhance project teams</td>
<td>A. Create formal application security support portal B. Establish role-based examination/certification</td>
</tr>
</tbody>
</table>
Per Level, SAMM defines...

- Objective
- Activities
- Results
- Success Metrics
- Costs
- Personnel
- Related Levels
SAMM Quick Start
**Assess**

SAMM includes assessment worksheets for each Security Practice.

<table>
<thead>
<tr>
<th>Education &amp; Guidance</th>
<th>Yes/No</th>
</tr>
</thead>
<tbody>
<tr>
<td>✤ Have most developers been given high-level security awareness training?</td>
<td></td>
</tr>
<tr>
<td>✤ Does each project team have access to secure development best practices and guidance?</td>
<td></td>
</tr>
<tr>
<td>✤ Are most roles in the development process given role-specific training and guidance?</td>
<td></td>
</tr>
<tr>
<td>✤ Are most stakeholders able to pull in security coaches for use on projects?</td>
<td></td>
</tr>
<tr>
<td>✤ Is security-related guidance centrally controlled and consistently distributed throughout the organization?</td>
<td></td>
</tr>
<tr>
<td>✤ Are most people tested to ensure a baseline skill-set for secure development practices?</td>
<td></td>
</tr>
</tbody>
</table>
Lessons Learned – Organisation Specific

• Pre-screen general software development maturity

• Define assessment scope in organisation:
  - Organisation wide
  - Selected Business Units
  - Development Groups (internal, supplier)
  - IT infrastructure Groups (hosting internal, cloud)

• Involve key stakeholders
  Invaluable for awareness & education

• Apply CONSISTENT (same interviewers) within same organisation
Lessons Learned - Interview / Scoring

• Adapt & select subset questionnaire per profile
  (risk management, development, IT infrastructure, ...)
• Try different formats: interview style, workshops
• Capture more details:
  "Adjusted" scoring
  Ask percentage instead of Yes/No
  If Yes: request CMM level for activity
  Ask about strengths & weaknesses
• Validate results:
  Repeat questions to several people
  Lightweight vs full approach
  Anonymous interviews
  Aggregate gathered information
Goal

- **Gap analysis**
  - Capturing scores from detailed assessments versus expected performance levels
- **Demonstrating improvement**
  - Capturing scores from before and after an iteration of assurance program build-out
- **Ongoing measurement**
  - Capturing scores over consistent time frames for an assurance program that is already in place
Goal - Lessons Learned

• Link to the organisational context
  - Specific Business Case (ROI)
  - Organisation objectives / risk profile

• Think carefully about target SAMM level
  - So you want to achieve all 3’s. (Hmm. Who are you, NSA?)
  - Link to industry level
  - Respect practice dependencies
  - It can make sense not to include particular low-level activities, or to lower a current level
Goal - Lessons Learned

• Get **consensus**, management support

• Be ready for **budget** questions (linked to Plan phase)
  - man days, CAPEX, OPEX
  - General stats about % impact overall budget

• Create & reuse own **organisation template** GOAL
Plan

• Roadmaps: to make the “building blocks” usable

• Templates for typical kinds of organizations
  • Independent Software Vendors
  • Online Service Providers
  • Financial Services Organizations
  • Government Organizations

• Tune these to your own targets / speed
Plan - Lessons Learned

• Identify quick wins (focus on success cases)
• Start with awareness / training
• Adapt to upcoming release cycles / key projects
• Spread effort & “gaps to close” over realistic iterations

• Spread work, roles & responsibilities
  SW security competence centre, development, security, operations
  For instance service portfolio and guidelines: when and who?
• Take into account dependencies

• Be ready to adapt planning
Plan - Budgeting

- Average budget impact 5%-15% on project
- Cost of tooling
  Central procurement vs per development group
- Cost of training
  Do not forget internal/external time spent
- Cost of external suppliers / outsourcing
- Different technology stacks will impact budget
Implement: 150+ OWASP resources
## Resources: Education & Guidance

<table>
<thead>
<tr>
<th>Education &amp; Guidance</th>
<th>EG 1</th>
<th>EG 2</th>
<th>EG 3</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Objective</strong></td>
<td>Offer development staff access to resources around the topics of secure programming and deployment</td>
<td>Educate all personnel in the software life-cycle with role-specific guidance on secure development</td>
<td>Mandate comprehensive security training and certify personnel for baseline knowledge</td>
</tr>
<tr>
<td><strong>Activities</strong></td>
<td>A. Conduct technical security awareness training</td>
<td>A. Conduct role-specific application security training</td>
<td>A. Create formal application security support portal</td>
</tr>
<tr>
<td></td>
<td>B. Build and maintain technical guidelines</td>
<td>B. Utilize security coaches to enhance project teams</td>
<td>B. Establish role-based examination/certification</td>
</tr>
</tbody>
</table>

- WebGoat
- iGoat, GoatDroid
- AppSec Tutorials
- Top Ten
- Development Guide
- Cheat Sheets
- Quick Reference Guide
- Education Testing Guide
- Hackademic Challenges
- Red Book
Implement – Lessons Learned

• Adapt & reuse SAMM to your organisation
• Categorize applications: High, Medium, Low based on risk: e.g. Internet facing, transactions, ...
• Recheck progress & derive lessons learned at each iteration
• Create & improve reporting dashboard Application & process metrics
• Treat new & legacy code bases differently

• Agile: differentiate between Every Sprint, Bucket & one-time AppSec activities
• Balance planning on people, process, knowledge and tools
Lessons Learned – AppSec Competence Centre

- Inject & spread best practices
- “market & promote” – do not become risk/audit function
- Do not become operational bottle-neck
- Spread/hand-over knowledge to champions throughout organisation
- Create & nurture AppSec community
SAMM Resources
owasp.org/index.php/samm

• Presentations
• Quick Start (part of SAMM v1.1)
• Assessment worksheets / templates
• Roadmap templates
• Translations (Spanish, Japanese, ...) **GERMAN upcoming**
• SAMM mappings to ISO/EIC 27034 – BSIMM – PCI (to be released)
• **NEW**: Training material (Cambridge)
Self-Assessment Online

https://ssa.asteriskinfosec.com.au
SAMM Roadmap

Build the SAMM community:
• Grow list of SAMM adopters
• Workshops at conferences
• Dedicated SAMM summit

V1.1:
• Incorporate Quick Start / tools / guidance / OWASP projects
• Revamp SAMM wiki

V2.0:
• Revise scoring model
• Model revision necessary? (12 practices, 3 levels, ...)
• Application to agile
• Roadmap planning: how to measure effort?
• ...
Critical Success Factors

• Get initiative buy-in from stakeholders
• Adopt a risk-based approach
• Awareness / education is the foundation
• Integrate & automate security in your development / acquisition and deployment processes
• Measure: Provide management visibility
Get involved

• Project mailing list / work packages
• Use and donate (feed)back!
• Donate resources
• Sponsor SAMM
OWASP SAMM Summit 2015
27-28 March 2015
Dublin, Ireland

Friday – User Day
• Talks
• Training
• Topic roundtables

Saturday – Project Day
• Publish SAMM v1.1
• Workshops
• Roadmap

owasp.org/index.php/OWASP_SAMM_Summit_2015
Follow OWASP SAMM

twitter.com/OwaspSA MM
Measure & Improve!

owasp.org/index.php/SAMM
Thank you!
## Mapping Projects / SAMM

<table>
<thead>
<tr>
<th>Project</th>
<th>Type</th>
<th>Level</th>
<th>SAMM Practice</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anti Samy</td>
<td>Code</td>
<td>Flagship</td>
<td>SA2</td>
<td></td>
</tr>
<tr>
<td>Enterprise Security API</td>
<td>Code</td>
<td>Flagship</td>
<td>SA3</td>
<td></td>
</tr>
<tr>
<td>ModSecurity Core Rule Set</td>
<td>Code</td>
<td>Flagship</td>
<td>EA2</td>
<td></td>
</tr>
<tr>
<td>CSRFGuard</td>
<td>Code</td>
<td>Flagship</td>
<td>SA2</td>
<td></td>
</tr>
<tr>
<td>Web Testing Environment</td>
<td>Tools</td>
<td>Flagship</td>
<td>ST2</td>
<td></td>
</tr>
<tr>
<td>WebGoat</td>
<td>Tools</td>
<td>Flagship</td>
<td>EG2</td>
<td></td>
</tr>
<tr>
<td>Zed Attack Proxy</td>
<td>Tools</td>
<td>Flagship</td>
<td>ST2</td>
<td></td>
</tr>
<tr>
<td>Application Security Verification Standard</td>
<td>Documentation</td>
<td>Flagship</td>
<td>DR2</td>
<td>ASVS-L4</td>
</tr>
<tr>
<td>Application Security Verification Standard</td>
<td>Documentation</td>
<td>Flagship</td>
<td>CR3</td>
<td>ASVS-L4</td>
</tr>
<tr>
<td>Application Security Verification Standard</td>
<td>Documentation</td>
<td>Flagship</td>
<td>ST3</td>
<td>ASVS-L4</td>
</tr>
<tr>
<td>Code Review Guide</td>
<td>Documentation</td>
<td>Flagship</td>
<td>CR1</td>
<td></td>
</tr>
<tr>
<td>Codes of Conduct</td>
<td>Documentation</td>
<td>Flagship</td>
<td>EG1</td>
<td>not applicable</td>
</tr>
<tr>
<td>Development Guide</td>
<td>Documentation</td>
<td>Flagship</td>
<td>EG1</td>
<td></td>
</tr>
<tr>
<td>Secure Coding Practices - Quick Reference Guide</td>
<td>Documentation</td>
<td>Flagship</td>
<td>SR1</td>
<td></td>
</tr>
<tr>
<td>Software Assurance Maturity Model</td>
<td>Documentation</td>
<td>Flagship</td>
<td>SM1</td>
<td>Recursiveness :-)</td>
</tr>
<tr>
<td>Testing Guide</td>
<td>Documentation</td>
<td>Flagship</td>
<td>ST1</td>
<td></td>
</tr>
<tr>
<td>Top Ten</td>
<td>Documentation</td>
<td>Flagship</td>
<td>EG1</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Project</th>
<th>Type</th>
<th>Level</th>
<th>SAMM Practice</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wapiti</td>
<td>Tools</td>
<td>Labs</td>
<td>EGI</td>
<td></td>
</tr>
<tr>
<td>Web Browser Testing System</td>
<td>Tools</td>
<td>Labs</td>
<td>ST1</td>
<td></td>
</tr>
<tr>
<td>WebScarab</td>
<td>Tools</td>
<td>Labs</td>
<td>ST1</td>
<td></td>
</tr>
<tr>
<td>WebSlayer</td>
<td>Tools</td>
<td>Labs</td>
<td>ST1</td>
<td></td>
</tr>
<tr>
<td>WSFuzzer</td>
<td>Tools</td>
<td>Labs</td>
<td>ST1</td>
<td></td>
</tr>
<tr>
<td>Yasca</td>
<td>Tools</td>
<td>Labs</td>
<td>CR2</td>
<td></td>
</tr>
<tr>
<td>AppSec Tutorials</td>
<td>Documentation</td>
<td>Labs</td>
<td>EG1</td>
<td></td>
</tr>
<tr>
<td>AppSensor</td>
<td>Documentation</td>
<td>Labs</td>
<td>EB3</td>
<td></td>
</tr>
<tr>
<td>AppSensor</td>
<td>Documentation</td>
<td>Labs</td>
<td>SA2</td>
<td></td>
</tr>
<tr>
<td>Cloud10</td>
<td>Documentation</td>
<td>Labs</td>
<td>EB1</td>
<td></td>
</tr>
<tr>
<td>CIF</td>
<td>Documentation</td>
<td>Labs</td>
<td>EG1</td>
<td></td>
</tr>
<tr>
<td>Fuzzing Code</td>
<td>Documentation</td>
<td>Labs</td>
<td>ST1</td>
<td></td>
</tr>
<tr>
<td>Legal</td>
<td>Documentation</td>
<td>Labs</td>
<td>SR3</td>
<td></td>
</tr>
<tr>
<td>Podcast</td>
<td>Documentation</td>
<td>Labs</td>
<td>EG1</td>
<td></td>
</tr>
<tr>
<td>Virtual Patching Best Practices</td>
<td>Documentation</td>
<td>Labs</td>
<td>EB3</td>
<td></td>
</tr>
</tbody>
</table>
## OWASP Projects Coverage

<table>
<thead>
<tr>
<th>Governance</th>
<th>Strategy &amp; Metrics</th>
<th>Policy &amp; Compliance</th>
<th>Education &amp; Guidance</th>
</tr>
</thead>
<tbody>
<tr>
<td>SM1</td>
<td>1</td>
<td>PC1</td>
<td>EG1</td>
</tr>
<tr>
<td>SM2</td>
<td>0</td>
<td>PC2</td>
<td>EG2</td>
</tr>
<tr>
<td>SM3</td>
<td>0</td>
<td>PC3</td>
<td>EG3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1</td>
<td>11</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Construction</th>
<th>Threat Assessment</th>
<th>Security Requirements</th>
<th>Security Architecture</th>
</tr>
</thead>
<tbody>
<tr>
<td>TA1</td>
<td>0</td>
<td>SR1</td>
<td>SA1</td>
</tr>
<tr>
<td>TA2</td>
<td>0</td>
<td>SR2</td>
<td>SA2</td>
</tr>
<tr>
<td>TA3</td>
<td>0</td>
<td>SR3</td>
<td>SA3</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>2</td>
<td>5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>DR1</td>
<td>0</td>
<td>CR1</td>
<td>ST1</td>
</tr>
<tr>
<td>DR2</td>
<td>1</td>
<td>CR2</td>
<td>ST2</td>
</tr>
<tr>
<td>DR3</td>
<td>0</td>
<td>CR3</td>
<td>ST3</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>5</td>
<td>22</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Deployment</th>
<th>Vulnerability Management</th>
<th>Environment Hardening</th>
<th>Operational Hardening</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM1</td>
<td>0</td>
<td>BH1</td>
<td>OE1</td>
</tr>
<tr>
<td>VM2</td>
<td>0</td>
<td>BH2</td>
<td>OE2</td>
</tr>
<tr>
<td>VM3</td>
<td>0</td>
<td>BH3</td>
<td>OE3</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>3</td>
<td>0</td>
</tr>
</tbody>
</table>

Total:
- Governance: 11
- Construction: 5
- Verification: 22
- Deployment: 3
SDLC Cornerstones (recap)

- People
- Process
- Knowledge
- Tools & Components
- Risk
- Training

- Roles & Responsibilities
- Standards & Guidelines
- Compliance
- Transfer methods
- Development support
- Assessment tools
- Management tools